Policy #: IT.007–Unacceptable Use Policy

Governed by: IT Administration
Approval Date: November 1, 2016 **Last Updated:** November 1, 2016
Purpose: CEO IT Systems Unacceptable Use

Unacceptable Use of CEO IT Systems

All CEO employees should use their own judgment regarding what is unacceptable use of CEO's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager prior to proceeding.

The following outlines examples of unacceptable use of CEO IT systems:

- All prohibited activities.
    - These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

- All activities detrimental to the success of CEO.
    - These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business.
    - These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

- All activities that are inappropriate for CEO to be associated with and/or are detrimental to the company's reputation.
    - This includes pornography, gambling, inciting hate, bullying and harassment.